

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF
A BLACK, SAMSUNG GALAXY J3
ORBIT, MODEL SM-S367VL(GP),
ASSOCIATED WITH TELEPHONE
NUMBER (603) 991-5718, BEARING
IMEI 352069100045458, CURRENTLY
LOCATED IN BEDFORD, NEW
HAMPSHIRE

Case No. 20-mj-24-AJ

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER
RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Shayne Tongbua, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been employed with the FBI since 2009. In the course of my duties, I have investigated national security matters relating to economic espionage and terrorism, as well as federal criminal violations concerning crimes against children, human trafficking, narcotics, organized crime, domestic terrorism, weapons of mass destruction, and other criminal violations. I have acquired experience in investigating various violations of federal law through extensive training at the FBI Academy in Quantico, Virginia, and by conducting investigations in the field. During my career,

I have participated in many criminal investigations as a case agent and/or in a subsidiary role and have participated in the execution of numerous federal search warrants.

3. I am a federal law enforcement officer of the United States within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), duly authorized to conduct investigations of and make arrests for violations of United States Code.

4. The probable cause set forth in this affidavit is based upon my personal knowledge and observations, experience and training, as well as through information derived from investigators of the Bethlehem, NH Police Department (PD), Exeter NH PD, Littleton NH PD, NH State Police, the FBI NH Resident Agencies, and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), cooperating associates and family members, database queries, and review of electronic evidence.

5. Since the affidavit is being submitted for the limited purpose of establishing that probable cause exists to support the issuance of a search warrant, I have not included details about every aspect of the investigation. While this affidavit contains all the material information I am aware of that is pertinent to the requested search warrants, it does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched is a black, Samsung Galaxy J3 Orbit, Model SM-S367VL(GP), associated with telephone number (603) 991-5718, bearing IMEI 352069100045458, seized on December 20, 2019 from the person of Johnathon IRISH in Littleton, NH, hereinafter the "Device," and any and all SIM cards or data storage cards installed

or contained within the Device. The Device is currently located at the FBI New Hampshire Resident Agency, 15 Constitution Drive, Bedford, New Hampshire.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

Background

8. Johnathon Irish was convicted of aiding and abetting the making of a material false statement in connection with the acquisition of a firearm and making a material false statement to a federal agent in *United States v. Irish*, case no. 13-cr-142-01-PB, District of New Hampshire. On February 19, 2015, Irish was sentenced for these offenses to a term of 18 months of imprisonment followed by 36 months of supervised release. As such, Irish is legally prohibited from possessing firearms.

9. During the investigation that led to Irish's federal convictions, the FBI took custody of three firearms that previously belonged to Irish: a Sig Sauer sig 516, 5.56 caliber AR-15 style rifle, serial number 53E001626; a Sig Sauer .45 caliber 1911 pistol, serial number GS34120, and a Sig Sauer .40 caliber 226 pistol, serial number UU610911. Those firearms were released to Roscoe Whitney. Whitney signed a stipulation stating that he would not allow Irish access to those firearms at any time, under any circumstances, as that could constitute a crime of aiding and abetting the possession of a firearm by a convicted felon. The stipulation is dated July 14, 2015.

Investigation

10. On December 26, 2018, Stephanie Irish (“Stephanie”), Irish’s wife, contacted the FBI Bedford Resident Agency and stated that Irish was in possession of a 1911 pistol and an assault rifle. She believed these to be the same firearms Irish owned previously, were seized by the FBI, and released to the care of Whitney.

11. On October 27, 2019, Stephanie provided the FBI with screen shots of text messages that she stated were between her and Irish. Stephanie explained the context of the conversation was in response to perceived harassment from her brother and mother. In the exchange, Irish sent the following messages:

- “Pull Romeo out make sure hes ready to play;”
- “Key box # 9020;”
- “Get Karma ready if you want.”

Stephanie relayed that “Romeo” is what Irish calls his 1911 handgun, and “Karma” is what he calls his M4 rifle. She also explained the lock code provided was to access the guns.

12. Investigators interviewed an individual named Neil Prive, who indicated he received a large black container directly from Irish in approximately late October 2019. Prive reported that he had been contacted by Haskell, who conveyed concern about Irish’s mental state and whether he might hurt himself or others. Prive reported that Irish also made similar statements about giving the guns to Prive, so he (Irish) “wouldn’t do anything stupid.” Prive stated that he was aware the box contained a rifle, a handgun, a shotgun, a tactical vest, and ammunition. Prive stated that he subsequently received a message from Irish by phone saying he had a buddy who would take the guns.

13. On November 11, 2019, FBI seized the following items from Gerald Roy: (1) a Sig Sauer 516, 5.56 NATO, Rifle [S/N: 53E001626]; (2) a Sig Sauer 1911, .45 Caliber, Pistol [S/N: GS34120];¹ (3) a Catamount Fury, 12 Gauge, Shotgun [S/N: CAT-002586]; and (4) miscellaneous ammunition & magazines, all of which were stored in a large black container. In an interview with FBI, Roy stated that Irish had recently called him to ask him to take his guns. Roy stated that he took possession of the firearms from another individual on November 17, 2019. Roy also allowed investigators to take photographs of the text messages on his phone, which included communications that Roy reported were between Roy and Irish, including the following:

- Multiple missed calls from Irish to Roy between October 31, 2019 and November 3, 2019;
Text messages from Irish to Roy, including: “Gary its Johnathon PLEASE CALL ME” on November 2, 2019, and “Gary sorry for the earl[y] hour, Stephanie will be making contact with Roscoe then presumably you to verify location, how long you had them, that you picked them up from Roscoe etc. Thank you” on November 25, 2019.

In addition, Roy reported that his phone also contained additional communications with Irish’s mother, Nancy Haskell, regarding signing documentation to show that Roy took custody of the firearms. Investigators obtained screen shots of these communications.

14. On November 25, 2019, Stephanie reported that Irish had communicated with her over the past month via phone and email and that in those communications he was reportedly trying to convince her that he was arranging the transfer of his guns.

¹ Two of the firearms seized from Roy, the Sig Sauer 516, 5.56 NATO, Rifle [S/N: 53E001626] and a Sig Sauer 1911, .45 Caliber, Pistol [S/N: GS34120], were firearms that had been seized from Irish in the earlier investigation and released to Whitney. *See, supra*, ¶ 9.

15. On December 18, 2019, a grand jury sitting in the District of New Hampshire returned an indictment charging Irish with the unlawful possession of firearms, in violation of 18 U.S.C. 922(g), in *United States v. Irish*, 19-cr-251-LM.

16. On December 12, 2019, Irish was arrested by members of the FBI NH Joint Terrorism Task Force (JTTF) pursuant to a federal arrest warrant. During a search for weapons and contraband, the Device was discovered on Irish's person. After being advised of his Miranda Rights, Irish waived his right to counsel and agreed to speak with investigators without an attorney present. During the interview, Irish indicated that documentation concerning the transfer of his firearms was located on the phone. He stated, "I have the paperwork in my email." Irish then gestured towards his phone, and said, "you want to see the paperwork?"

17. The Device is currently in storage at the FBI New Hampshire Resident Agency, 15 Constitution Drive, Bedford, New Hampshire. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or

traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video,

or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing

computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address

so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- c. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

- d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

/s/ Shayne Tongbua
Shayne Tongbua
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on January 14, 2020 at Concord, New Hampshire.

Andrea K. Johnstone
Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

The property to be searched is a black, Samsung Galaxy J3 Orbit, Model SM-S367VL(GP), associated with telephone number (603) 991-5718, bearing IMEI 352069100045458, seized on December 20, 2019 from the person of Johnathon IRISH in Littleton, NH, hereinafter the “Device,” and any and all SIM cards or data storage cards installed or contained within the Device. The Device is currently located at the FBI New Hampshire Resident Agency, 15 Constitution Drive, Bedford, New Hampshire.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 922(g)(1) and involve Johnathon Irish since, including:
 - a. Information related to firearms, including the acquisition, possession, and disposition of firearms, including communications, photographs, videos;
 - b. Information (including names, addresses, phone numbers, or any other identifying information) regarding any individuals who communicated with the user of the phone regarding firearms;
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or

copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.